Call for expressions of interest to select entities in Member States that provide the necessary facilities to host and operate National SOC Platforms/ National Cyber Hubs

1. Introduction 1
2. Objectives of the national SOC platforms 2
3. About this call for expressions of interest (CfEI) 4
4. Content of the applications 7
4.1. Submission forms 7
4.2. Key features of National SOC platforms 8
5. Eligibility and award criteria 10
6. Overview of the assessment and selection procedure 12
6.1. Assessment procedure 12
6.2. Selection 13
6.3. Communication 13
7. Tentative timetable 14
8. Procedure for the submission of expressions of interest 14
Annexes 15
List of abbreviations 16

1. Introduction

In a context of accelerated digitisation together with a growing number cybersecurity incidents with increasing impact, in December 2020 the European Commission (EC) adopted the "EU cybersecurity strategy for the Digital Decade"[1]. Among other objectives, the cybersecurity strategy aims to improve capacities and cooperation to detect more cyber threats, more quickly, before they can cause large-scale damage.

The Russian invasion of Ukraine further underlines and reinforces the need to urgently step up cybersecurity capabilities at national and at EU level. This requires intensifying the exchange of information and improving detection of cybersecurity threats so as to promote better situational awareness and inform preventive and response actions.

The EU cybersecurity strategy envisages building, strengthening, and interconnecting, across the EU, security operation centres (SOCs) and cyber threat intelligence (CTI) capabilities for monitoring, detection and analysis, with the aim of supporting the detection and prevention of cyber threats and the provision of timely warnings to authorities and all relevant stakeholders.

Such cyber security capabilities are typically ensured by SOCs[2] of public and private entities, in combination with computer emergency response teams / computer security incident response teams (CERTs/CSIRTs) with the support of external, specialised sources of intelligence on cyber threats.

To implement this strategy, the previous DIGITAL work programme (WP) for 2021-2022 included capacity-building actions for SOCs. The 2023 – 2024 WP aims at strengthening EU actions by supporting the creation of national SOCs, and networking them at European and EU level via cross-border SOCs and coordinating their activities to create a stronger SOC ecosystem, which will include local and regional, private and public security operational centres for both horizontal and vertical sectors.

As per the political agreement on the Cyber Solidarity Act[3] to be adopted and published in the Official Journal in autumn 2024, it is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the EU and to strengthen solidarity by enhancing Member States' and the EU's preparedness and ability to prevent and respond to significant, large-scale and large-scale-equivalent cybersecurity incidents.

The Cyber Solidarity Act envisages, as part of the European Cybersecurity Alert System, the establishment of a pan - European network of cyber hubs, to build and enhance coordinated detection and common situational awareness capabilities. It includes support for the development and consolidation of the national cyber hubs and the cross-border cyber hubs, also referred to as national SOCs/cross-border SOCs.

For the purpose of this call for expressions of interest, national SOCs could also be referred to as national cyber hubs and cross-border SOCs could be referred to as cross-border cyber hubs.

In this regard, under the EU's 'DIGITAL' funding program, EUR 89 million are dedicated to "Security Operation Centres"[4] in the cybersecurity work programme (WP) 2023-2024. One of the key actions envisaged is building and strengthening national SOCs, which play a key role as hubs or gateways to other SOCs at national level.

Where a Member State decides to participate in the European Cybersecurity Alert System, it must designate or, if necessary, establish a national cyber hub/national SOC. These national SOC platforms should be able to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and to contribute to a cross-border cyber hub/cross – border SOC platform. This should serve to improve detection capabilities and ultimately the prevention of and response to cyber threats and incidents.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018
[2] SOCs potentially cover any entity or team tasked with detecting and acting on cyber threats.
[3] https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1332
[4] https://ec.europa.eu/newsroom/dae/redirection/document/100739

The purpose of this call for expressions of interest (CfEI) is to select entities in EU Member States and other eligible countries[5], intending to participate in the European Cybersecurity Alert System and willing to deploy and manage national SOC platforms.

The single entity, designated or established as the national SOC/national cyber hub, selected following this CfEI will engage in joint procurement with the ECCC to purchase the necessary tools, infrastructures and services to create or strengthen the national SOC platform. For each joint procurement the EU will contribute up to 50% of the purchasing costs. The number of joint procurements to be conducted will depend on the number of successful applications from national SOCs/national cyber hubs selected following evaluation of this CfEI. The overall budget for procurement will be up to EUR 15 million.

Separately, a platform has to apply to receive a grant to complement the joint procurement(s). The related grant will be awarded if the relevant requirements in the separate call for proposals are met and only if the application in response to this call for expressions of interest is successful. The EU will contribute up to 50% of eligible costs, such as staff costs or other eligible costs for setting up and running the national SOC platform, its interaction and cooperation with other stakeholders, with the exception of those tools, infrastructures and services that will be purchased through the joint procurement(s). The grant funding for the eligible costs of the national SOC platforms will come from the call for proposals on national SOCs, for which there is a total amount of EUR 5.8 million.

The deployment of these national platforms is a pivotal component in a wider strategy and set of actions aimed at the stepping – up of monitoring and detection capabilities and the improvement of situational awareness at national, cross-border and EU level, and at paving the way for building a **collaborative, interoperable and sustainable pan-European network of infrastructure.** The network of infrastructure will link SOC entities designated at national level forming several cross-border SOC platforms, which will be able to build up shared capacities and exchange information among themselves. Such platforms would together constitute a pan-European network of infrastructure.

Cooperation and exchange of information will be encouraged among the various entities at all levels through the **procurement of common equipment, software and services**, the development of **cooperation frameworks** and of specific conditions to ensure a high level of **interoperability** among the supported projects and infrastructures, which will fit into a **common, high-level blueprint architecture**.

In this regard, national SOCs must share information with other stakeholders in a mutually beneficial exchange of information and commit to applying to participate in a cross-border SOC platform within the next 2 years from the date on which the tools, infrastructures and services were acquired, or which it received grant funding, whichever occurred sooner, with a view to exchanging information with other national SOCs.

2. Objectives of the national SOC platforms

The **general objective** of "**national SOC platforms/cyber hubs**" is to act as reference points and gateways to other public and private organisations at national level for participation in the European Cybersecurity Alert System and to ensure that cyber threat information from public and private entities is shared and collected at national level in an effective and streamlined manner.

National SOCs are public entities given the role at national level to act as clearinghouses for detecting, gathering, aggregating and storing data on cybersecurity threats, analysing this data, and sharing and reporting cyber threat intelligence (CTI), reviews and analyses. They provide a central operational capacity and support other SOCs at national level (e.g., by offering guidance or training, making available data or analysis of this

[5] EEA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States

data, coordinating joint detection and monitoring actions, providing incident response services methodologies towards the mitigation of identified threats, vulnerabilities and/or misconfiguration weaknesses). They will play a central role at national level and can act as a hub within a context of SOCs in the different countries.

The platforms should act as a central national point allowing for broader pooling of relevant data and CTI, enable the large scale dissemination of threat information on a large scale and among a large and diverse set of actors (e.g., CERTs/CSIRTs, ISACs, operators of critical infrastructures).

National SOC platforms will contribute to enhancing and consolidating collective situational awareness and capabilities in detection and CTI. They will support the development of better performing data analytics, detection, and response tools, through the pooling of larger amounts of data.

The National SOC platforms should achieve this general objective through the following specific objectives:

- **Producing high quality, actionable information and CTI** through the use of state-of-the art tools and advanced tools and technologies (for example artificial intelligence (AI), including machine learning (ML) tools) on the large data sets of collected CTI.
- **Contributing to better detection and response to threats.** They should support quicker detection of cyber threats and incidents and more effective action plans and responses by relevant entities.
- **Contributing to collective situational awareness.** The platforms should contribute to the strengthening of the EU's common situational awareness and enhanced coordinated detection capabilities by sharing information at three levels:
    - At national level. Close and coordinated cooperation between public and private entities is central to strengthening the EU's resilience in the cybersecurity sphere. National SOCs could strengthen cooperation and information sharing between public and private entities and, as part of this, request and receive specific information where appropriate and in accordance with national and EU law. Different levels of sharing and integration of data and tools can be envisaged, ranging from the exchange of intelligence feeds and indicators of compromise (IoC) to more contextualised or sophisticated information on threats, incidents, and vulnerabilities.
    - Between national SOC platforms. National SOCs must share information with other national SOCs and commit to applying to participate in a cross-border SOC platform within the next 2 years. Conditions for exchanging information with other platforms are to be established. As per de political agreement on the Cyber Solidarity Act to be published in autumn 2024, entities participating in the European Cybersecurity Alert System should ensure a high-level of interoperability among themselves including, as appropriate, as regards data formats, taxonomy, data handling and data analysis tools, and secure communications channels, a minimum level of application layer security, situational awareness dashboard and indicators.
    - With relevant EU entities and networks. Platforms should provide an adequate level of information to responsible networks and entities at EU level, in defined situations (such as in case of major incidents) and subject to appropriate conditions, in order to support common situational awareness and effective crisis management and response. In particular, platforms should support the exchange of relevant data and information with relevant sectoral and cross-sectoral communities, including relevant industry information sharing and analysis centers ('ISACs'). If the national cyber hub/SOC platform is not the competent authority designated or established by the relevant Member State under Directive (EU) 2022/2555, it is crucial that it coordinates with that competent authority in respect of such data requests and receipt.
- **Improving EU technological sovereignty.** The platforms should enhance the EU's cyber-threat knowledge base, support the development and improvement of EU tools, and help create and structure a European ecosystem for sharing CTI.
- **Providing other services and activities.** Such services and activities could include the sharing of tools (including commonly procured tools), the creation of one or more data lakes, the provision of cyber range services, and/or the training of cybersecurity analysts. These services could be offered, for

example, to the SOC network at national level, national critical infrastructures in the public and private sectors, CSIRTs, ISACs and where possible, to the wider EU cybersecurity community, including EU industry and research and academia.

3. About this call for expressions of interest (CfEI)

The purpose of this CfEI is to select entities in the Member States that can provide the necessary facilities to host and operate the national SOC/national cyber hub. The call for expression of interest will also build up the planning and design of necessary tools, infrastructures and services to be jointly purchased.

3.1 Selection of national SOCs/cyber hubs

This CfEI intends to select entities **designated or established by the Member States as national SOC/cyber hub**.

For the purpose of this CfEI, a national SOC is understood to be a public body that acts as a central hub, having the operational capacity to act as a reference point and gateway to other public or private organisations that themselves have significant capacities to produce, share, receive and analyse cybersecurity related data (e.g., operators of critical infrastructures, cybersecurity companies), or organisations that benefit from the services of the national SOC. The national SOC/cyber hub may be a CSIRT, or where applicable, a national cyber crisis management authority or other competent authority designated or established under Directive (EU) 2022/2555, or another entity.

Hosting and usage agreements will be signed between the selected national SOCs and the ECCC regulating the usage of the tools, infrastructures and services.

While the applicants under this CfEI are the entities designated or established by the Member States as national SOC/cyber hub, identification and engagement of the relevant stakeholders should be envisaged. To this end, National SOC platforms should aim at involving a large number of **contributors**, i.e. entities willing to contribute to the objective of the platforms, in particular by sharing data and tools, but without a direct link to the governance and operation of the platforms. The relevant contributors for a national SOC/cyber hub could be, among others: sectoral SOCs, national decision and policy makers as well as other governmental and non-governmental organisations, law enforcement, academic, research and innovation communities, private sector including the sectors of essential and important entities according to the NIS2 Directive.

While the European Cybersecurity Alert System is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructures.

3.2 Overview of the process

In response to this CfEI, applicants should submit a proposal that explains how the national SOC platform will be created or strengthened. The application should explain in detail the goods and services that the participating national SOC intends to jointly procure with the ECCC in order to create or strengthen the national SOC platform.

To this end, each application should provide a detailed description of the proposed approach using the submission forms attached to this document:

- the submission form on 'information about the applicant' in Annex 1
- the submission form for the expression of interest related to the joint procurement(s) in Annex 2.

The submission of an expression of interest to engage in joint procurement with the ECCC for the purchase of goods and services necessary to create or strengthen a national SOC platform will be evaluated using the evaluation criteria established in this document.

Separately, applicants have to submit a proposal for a grant to fund running costs and other costs of the national SOC platform, which will be evaluated using the evaluation criteria established in the relevant call document under the Digital Europe Programme[6].

The procedure for creating or strengthening a national SOC platform with the support of funding provided under this call for expressions of interest and the relevant call for proposals[7] will be as follows:

1. This call for expressions of interest will lead to the selection of applicants intending to create or strengthen a national SOC platform.
2. Before launching the procedure for the acquisition of the tools, infrastructures and services, the ECCC and the national cyber hub/national SOC will conclude a hosting and usage agreement. This agreement will set out practical arrangements for managing the hosting and usage of the tools infrastructures and services co-owned by the ECCC and the participating national SOC after joint procurement has been carried out.
3. Each selected national cyber hub/national SOC will take part in joint procurement of goods and services with the ECCC. Several parallel joint procurements procedures may thus be launched depending on the number of successful applications to CfEI. To this end, the ECCC and each selected Member State will sign a joint procurement agreement setting out the practicalities of the procurement procedure. The Member State must transfer the required budget to the ECCC.
4. The national cyber hub/national SOC will also apply for a complementary grant, to cover eligible costs, such as the cost of setting up and running the national SOC platform. To be eligible for such a grant, applicants must submit a proposal for a grant in response to the relevant call for proposals opened on 4 July 2024, following the procedure established for that purpose.

   By submitting an application in response to the CfEI, the national cyber hub/national SOC agrees to the terms and conditions set out in the model hosting and usage agreement. The model hosting and usage agreement is found in Annex 3 to this CfEI. The model hosting and usage agreement may be further modified before the close of the call for expressions of interest, subject to further discussions with Member States.

Member States willing to create or strengthen national SOC platforms/national cyber hubs will be selected through this call for expressions of interest.

For the joint procurement(s), the EU financial contribution is estimated at a maximum of EUR 15 million for all selected national SOC platforms/national cyber hubs. The EU contribution would cover up to 50% of the purchasing costs of the tools, infrastructures and services. The remaining procurement costs would be covered by the Member State. The EU contribution can only be used for jointly purchased goods and services.

In addition, Member States have to apply for a grant to cover other costs through a separate call for proposals[8]. The EU funding rate for such a grant is 50%.

Successful applicants to both workstreams (call for expressions of interest and call for proposals) will engage in joint procurement with the ECCC to purchase the necessary tools, infrastructures and services to create or strengthen the national SOC platforms/national cyber hubs.

To that end, the ECCC will conclude a hosting and usage agreement only with the national SOC platforms/national cyber hubs that are selected following this CfEI and that have been awarded a grant under the call DIGITAL-ECCC-2024-CYBER-07-SOC. This condition is cumulative.

Joint Procurement(s)

[6] See section DIGITAL-ECCC-2024-CYBER-07-SOC - National SOCs in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)
[7] See section DIGITAL-ECCC-2024-CYBER-07-SOC – National SOCs in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)
[8] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2024/call-fiche_digital-eccc-2024-deploy-cyber-07_en.pdf

The financial rules of the ECCC, adopted through DECISION No GB/2023/1[9] of the ECCC Governing Board, set out the conditions under which the ECCC may engage in procurement, including joint procurement with the Member States.

Joint procurement(s) for tools, infrastructures and services to create or strengthen national SOC platforms will be carried out by the ECCC (or the Commission acting on behalf of the ECCC until the ECCC becomes financially autonomous) in accordance with the ECCC financial rules and using the ECCC procedural provisions. The ECCC will jointly acquire, with each national cyber hub/national SOC selected further to the CfEI, relevant components of a national SOC platform and will co-own them with the participating Member State that provides a share of the funding. Share of ownership will correspond to share of the funding provided.

The designated or established national cyber hub/National SOC will represent the Member State and be authorised to sign the hosting and usage agreement, the joint procurement agreement and subsequent amendments to both agreements, if needed. **Evidence of this designation must be provided as part of the application in response to the CfEI.**

Each Member State must commit to transferring to the ECCC its individual share of the co-funding of at least 50 % of the overall estimated procurement costs not covered by the EU contribution. **Evidence of this commitment must be provided as part of the application in response to the CfEI.**

By submitting the application, applicants provide their prior acceptance with the terms and conditions set out in the model hosting and usage agreement. The model hosting and usage agreement is found in Annex 3 to this CfEI.

As part of their application, applicants are required to supplement the model hosting and usage agreement by completing the part of the agreement that is specific to their application. In particular, applicants must submit as part of their application a completed version of the model hosting and usage agreement.

Typical examples of goods and services to be procured include (indicatively):

- Hardware: servers, micro data center racks, high speed switches, firewall switches, GPUs, HSMs, probes;
- Software: visualisation tools, SIEM tools, vulnerability managers, aggregation tools, incident reporting tools, situation awareness correlator tools, AI/ML tools, PKI tools, orchestration systems;
- Services: CTI feeds, AI/ML functionality updates, dedicated service virtual telco line, cloud storage, software development and tuning services, consultancy services.

The objective is to encourage convergence among the various platforms and, as far as possible, to use procurement(s) to acquire goods and services that can benefit all the platforms by setting the path towards interoperability in the framework of cross-border cooperation and information exchange between the national SOCs/cyber hubs. If duly justified, specific types of goods and services for individual platforms could also be included in the procurement(s).

Rules for participation in DIGITAL Programme

In accordance with the Digital Europe Regulation, the joint procurement to be carried out following this CfEI **is restricted in line with the rules for participation in the Digital Europe Programme (DEP)**. The conditions set out in Appendix 3 - Implementation of Article 12(5) Regulation (EU) 2021/694 to the work programme 2023 – 2024[10] apply in this regard.

3.3 Applications for complementary grants

[9] https://cybersecurity-centre.europa.eu/system/files/2023-04/ECCC%20Decision%20No%201%20GB%202023_ECCC%20Financial%20Rules.pdf

[10] https://ec.europa.eu/newsroom/dae/redirection/document/100739

Separately from this call for expressions of interest, the selected national cyber hubs/national SOCs have to apply to be supported through grants awarded further to the call for grant proposals on national SOCs mentioned above. Procedures are described in the relevant call document[11].

Examples of specific activities which may be supported under the grant are provided in the text of that call for grant proposals on creating or strengthening national SOC platforms[12], whereas the eligible costs are defined in the general model grant agreement of the Digital Europe Programme.[13] Eligible costs may include the costs for maintenance or recurrent licences required for running the national SOC and which cannot be purchased as part of the joint procurement(s).

Grants may cover up to 50% of eligible costs of the selected national SOCs for setting up/strengthening a National SOC and running it.

Applications to receive such a grant must be submitted separately through the Funding and Tenders portal.[14]

Applications have to be made to both workstreams (call for expressions of interest for joint procurement and call for proposal for complementary grant). **Applicants to both workstreams must be the same entities designated or established as national SOCs/cyber hubs. Grants will only be awarded to applicants that have succeeded in the evaluation of the joint procurement action.**

Any application for a grant by entities also applying to this call for expressions of interest should be consistent with the application to engage in joint procurement under this call for expressions of interest, notably by ensuring complementarity and avoiding duplication of costs to be covered.

4. Content of the applications

4.1. Submission forms

Participants must fill in the submission forms in Annex 1 and 2 to describe their projects and enable their assessment.

1) The first Annex "Information on the participant" must provide administrative **details about the entity designated or established** by the Member State as national cyber hub/national SOC, including contact details and legal representatives.

2) The second Annex ("Information on the expression of interest") relates to the Joint procurement(s) and should be completed with:

- A **description of the project and its relevance and impact,** according to the key features detailed below in Section 4.2. Participants are expected to describe each part according to the points indicated.

- Information about the total cost of acquisition. This should include detailed **information about the types of goods and services to be procured under the joint procurement(s) for the purpose of creating/strengthening the national SOC platforms/national cyber hubs and their projected costs.**

- Information about existing infrastructures and other resources offered by those replying to the CfEI.

- A short description of complementarity with the application for grants. Applicants should provide a summary of the grant part of the project and explain the link between the procurement and the grant parts, explaining how one complements the other and which aspects and costs they cover respectively.

[11] See section DIGITAL-ECCC-2024-CYBER-07-SOC - National SOCs in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)
[12] See section DIGITAL-ECCC-2024-CYBER-07-SOC - National SOCs in the call-fiche_digital-eccc-2024-cyber-07_en.pdf (europa.eu)
[13] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/agr-contr/mga_dep_en.pdf
[14] Funding & tenders (europa.eu)

4.2. Key features of National SOC platforms

This section describes the main features of the national SOC platforms/national cyber hubs, as background information when completing the submission form.

Several national SOC platforms/national cyber hubs will be selected following this CfEI, one in each Member State and other eligible countries. An appropriate level of synergies and collaboration will be required between them and/or with other national/cross-border platforms. In particular, the national SOC platforms should adopt consistent and interoperable approaches and standards, in order to allow for possible exchanges of information among them at a later stage and participation in a cross-border SOC platform, as appropriate. The requirements of the Cyber Solidarity Act (to be adopted and published in the Official Journal in autumn 2024) should be observed in this regard. The platforms should be congruent with the high-level blueprint architecture available in Annex 5.

Specifically, the submissions should cover the following elements:

- **General concept and organisation.** This section should explain the overall vision for the platform, including its maturity and readiness to host and operate the national SOC platform/national cyber hub. It should describe organisational aspects and demonstrate how these would enable increased data sharing and better detection capability for cyber threats. The overall setting should be designed to foster engagement and trust with other SOCs and relevant entities in the country. Proposals should also consider how the proposed platforms will help expand the EU's cyber threat knowledge base and make the EU more and technologically independent, also in view of a role in the cross-border platforms.
    - **Minimum condition for the expression of interest.** As set out above, a national SOC platform should be managed by the single entity acting under the authority of a Member State designated or established as the national cyber hub/ national SOCs (public entity acting as hub). This overall concept should constitute the common baseline for all submissions, however each platform can, within that context, take into account their specific focus. Basic conditions for collaboration with the relevant identified stakeholders should be outlined in the submission. While the platforms will be managed by public entities, a concrete engagement from the private sector, or at least a clear strategy to engage with the private sector, should be demonstrated from the outset.
    - **Objective to be achieved during the deployment phase.** A comprehensive governance framework should be developed. It should address data sharing (see below), security and access rights, collaboration conditions.
- **Interoperability of national SOC platforms at national and EU level:**
    - **Minimum condition for the expression of interest.** Standards and tools to be used within individual platforms should be described, and should be congruent with the common, high-level blueprint architecture described in Annex 5. The use of malware information sharing platform (MISP) and of the relevant state of the art IT tools is strongly recommended.
    - **Objective to be achieved during deployment phase.** Given that cross-border SOCs are required to agree on a single common data format and taxonomy and on a common data structure, to ensure interoperability and enable data sharing across platforms, national SOCs should also consider this choice in order to be ready for sharing or joining a cross-border consortium in the future. Other elements to consider include interoperable privacy preserving technologies, data handling tools, communication and security technology, and situation awareness dashboard and indicators.
- **Data management (level of data sharing, conditions and incentives and legal aspects)**
    - **Minimum condition for the expression of interest**. National cyber hubs/SOCs should demonstrate a willingness to share as much information as possible with the due level of speed and quality. A general approach to data ownership and management, including legal aspects should be outlined. The approach should ensure "compliance by design" with respect to relevant EU and national legislations, in particular as regards rules on data protection and privacy.

- **Objective to be achieved during deployment phase.** As part of the comprehensive concept and organisation framework referred to above, clear and appropriate rules of engagement should be drawn up so as to incentivise the various stakeholders/contributors to engage and share information. This should include detailed terms of reference, covering aspects such as data sharing (ownership, control, compliance, management), security and access rights. Also, engagement could be based on a set of indicators to measure stakeholder's participation in terms of the amount of information shared, frequency, quality and type of information, and a set of corresponding rewards (e.g., access to more detailed info). If several platforms are selected the ECCC may invite them to share best practices, in which case they should join a working group to do so. Applicants are invited to include such tasks in the grant part of their proposal.

- **Contribution to national and EU-level situational awareness:**
  - **Minimum condition for the expression of interest.** The national SOC platform should be the national reference point for cybersecurity situational awareness. As outlined in the blueprint architecture in Annex 5, it is a single point of contact towards other national SOCs and the cross-Border SOC in which it may participate, thus contributing not only to the national but also to the EU common situational awareness and coordinated detection capabilities. To support situational awareness and effective crisis management and response, the national SOC platform should provide an adequate level of information to responsible networks and entities at national and EU level, in defined situations (such as in case of major incidents) and subject to appropriate conditions.. To specify what situations and conditions should be taken into account, the national SOC platform should engage with other platforms and the EU level. The national SOC/ cyber Hub needs to commit to apply to participate in a cross-border SOC platform within the next 2 years from the date on which the tools, infrastructures and services were acquired, or which it received grant funding, whichever occurred sooner.

- **Highly secure infrastructure and state-of-the-art technologies and tools:**
  - **Minimum condition for the expression of interest.** Candidates should describe dedicated secure infrastructure with the highest security standards. They should list equipment, software and services to be procured, which should include state-of the-art technologies, including notably AI/ML tools, based on a review of latest technologies available on the market. Proposals should be congruent with the common, high-level blueprint architecture described in Annex 5. With regard to secure communications, to ensure future interoperability across the different platforms, all candidates are invited to look at the suggested approach described in Section 4 of Annex 5. Proposals should also consider to what extent the proposed platforms will contribute to increase national and EU technological independence.
  - **Objective to be achieved during tender preparation phase.** The national SOCs/national cyber hubs selected following this CfEI will be required to work together with the ECCC on the preparation of the tender specifications for the procurement procedures. For this, working groups could be set up to consider a common approach to identifying needs. This effort will aim at identifying common equipment, tools, etc. to be purchased through the joint procurement actions, where possible (also in view of national SOCs aiming to join new or existing cross-border platform). As regards security and secure communication channels, entities should commit to meeting very high standards (if necessary, in a gradual way), considering also putting in place measures for the future evolution of cryptographic implementations towards post-quantum cryptography.

- **Provision of other services and activities to strengthen national and EU detection capabilities:**
  - **Minimum conditions for the expression of interest.** Candidates should describe other activities and services that could be provided by the platform. Such activities and services could include the sharing of tools (including commonly procured tools), the creation of one or several data lakes to train tools, the provision of cyber range services, and/or training of cybersecurity analysts. Depending on the activities and conditions agreed on by platforms, these services could be offered to the SOC network at national level, and where possible, to

the national and EU cybersecurity community, including industry and research and academia. In addition, links with existing and future relevant initiatives and projects benefiting from EU funding should be encouraged.

- **Objective to be achieved during the deployment phase.** The national SOCs/national cyber hubs selected following this CfEI will be encouraged to work together with the relevant stakeholders/contributors to identify synergies between other services and activities provided by individual platforms and to create appropriate infrastructures to leverage the shared pool of knowledge among the national SOC network. For this, they could for instance explore the possibility of creating one or more data lakes (see Section 2 above).

5. Eligibility and award criteria

In order to be eligible, the expression of interest for the joint procurement(s) must satisfy all the conditions set out below:

Expression of interest

1. The **expression of interest** must be submitted by the deadline given in Section 7, following the procedure set out in Section 8.
2. The **expression of interest** must be completed using the submission forms detailed in Annex I and Annex 24 addressing all mandatory aspects that are described in this document.
3. The **expression of interest** must be aligned with the objectives of this CfEI and fit into the expected approaches and elements of structure of national SOC platforms/national cyber hubs as described in Section 20.
4. The **expression of interest** must comply with the available budget detailed in Section 3.

Member State public body submitting the expression of interest

1 A national SOC platform/national cyber hub must be represented for legal purposes, including for submitting the expression of interest, by the single public entity acting under the authority of a Member State designated or established as the national cyber hub/national SOC.

2 The applicant must have legal personality and must be designated by the Member State to act as national cyber hub/national SOC. **Each application must contain the relevant documents proving the legal status of the national SOC/national cyber hub (e.g. designation letters, establishment act).**

3 Each Member State must provide a commitment to engage in a joint procurement action with the ECCC and to transfer the required acquisition costs. For this purpose, each application must contain copies of Annex 4 ('Commitment letter').

Failure to comply with those eligibility criteria will lead to disregarding the **expression of interest**.

Award criteria: Proposals must address all features indicated in this Section 0and will be assessed accordingly, taking into consideration the criteria indicated below for each of those features.

Award criteria for the expression of interest

Criterion	Score
General concept and governance:	0-20 points

• Quality of the vision, development plans and capability of the Member State to set up/strengthen and manage the national SOC platform/national cyber hub and to create a trusted environment stimulating the active participation of and sharing with relevant stakeholders. • Added value with relation to existing structures • Contribution to the EU's technological independence (e.g., use of EU made solutions, EU sourced data) • Sustainability of collaboration in the longer term • Feasibility and credibility of the presented approach	
Feasibility and quality of the interoperability: • Use of common data format and taxonomy • Quality of the proposed approach for interoperability and trusted interaction and data exchange with the national SOC network, other national SOC platforms and relevant EU stakeholders. Use of international recognised standards, protocols, best practices and guidelines to guarantee interoperability with other SOC platforms, including other national SOC platforms, and commitment for cross-platform cooperation and/or integration plans.	0-15 points
Highly secure infrastructure and state-of-the-art technologies and tools • Quality and effectiveness of the proposed plan for the readiness of the site to host the system • Security of the infrastructure • Use of most advanced technologies and tools based on market review • Compliance with the system specifications set out in this CfEI • Quality and pertinence of the current and proposed hosting facility's physical and IT infrastructure, its security, and its connectivity • Quality and pertinence of experience and know-how of the intended team that would be in charge at hosting entities for installing and running the platform	0-15 points
Data management • Quality and effectiveness of proposed plan for data management (e.g., access rights, ownership, control) • Commitment to share information with identified stakeholders/contributors at national level • Mechanisms to encourage data sharing by all contributors to the platforms • Approach to legal aspects (e.g., compliance with legislation, anonymisation, etc.)	0-15 points
Contribution to EU-level situational awareness • Commitment to contribute to EU situational awareness and to engage with the EU level to define minimum level of sharing of information with responsible EU entities (and other platforms, upon agreement).	0-15 points

• Feasibility and credibility of the proposed plan to apply for joining a cross – border SOC platform/cyber hub.	
Provision of other services and activities to strengthen EU detection capabilities • Quality and effectiveness of the proposed services and activities to contribute to EU capabilities • Links with existing and future relevant EU-funded initiatives and projects	0-10 points
Goods and services to be procured and total cost of acquisition (TCA) • Suitability of proposed goods and services to be jointly procured to achieve the objectives of the national SOC platform • Clarity and effectiveness of the estimated TCA of the national SOC platform, focusing on the total cost of what will be needed to be procured under the joint procurement(s) to run the platform	0-10 points

The threshold for each criterion is the 60% of the maximum available points attributed to the criteria itself. The total score will be calculated as the sum of the individual scores. The total maximum number of points is 100.

6. Overview of the assessment and selection procedure

The ECCC is responsible for assessing of the expressions of interest received. It will organise the submission and assessment procedures and communicate with those who submitted expressions of interest.

6.1. Assessment procedure

The submitted expressions of interest will be assessed in a procedure by a panel of ECCC staff and possibly assisted by independent experts. The ECCC will assess the eligibility and award criteria according to the sections above.

Only eligible expressions of interest will be assessed.

- Individual assessments. In the first step, each expression of interest will be assessed individually against the assessment criteria described in Section 5, receiving a score for each criterion, with explanatory comments. These scores and comments will be recorded in individual reports which form the basis for further assessment.
- Consensus meetings. After carrying out their individual assessment of the expressions of interest, the members of the evaluation committee will hold a consensus meeting, to agree on a common position, including comments and scores and prepare a consensus report.
- Panel review. The members of the panel will review the scores and comments for all expressions of interest to check for consistency across the assessments. If necessary, it will propose a new set of scores or revised comments and resolve cases where there are different views. The panel will prepare an assessment report, with its final ranking list and scores for the award criteria set out in Section 5. Only expressions of interest that score above threshold for each individual criterion will be ranked in order of the total score.
- Potential priority order. If necessary, a priority order for expressions of interest with the same score will be determined in the ranked list, according to the following approach: Expressions of interest with the same total score will be prioritised according to the scores they have received for the award criterion "*stakeholder engagement and Incentives*". If these scores are equal, priority will be based on the scores for the award criterion "*data management"*. If these scores are also the same, the panel will decide on the method used to assign priority, such as one of the other award criteria or, if all scores are equal, on other aspects of the expressions of interest.

6.2. Selection

The Executive Director of the ECCC will review the results of the assessment panel and will draw up a final ranking list based on the list proposed by the panel. The Executive Director may suggest to the authorising authority (i.e., the European Commission before the ECCC becomes financially autonomous, and the ECCC Governing Board afterwards), to deviate from the ranking proposed by the panel with a justification.

This final ranking list will consist of:

1. A main list with the expressions of interest to be selected as proposed by the experts complemented by any suggestion for deviation from this list as proposed by the Executive Director.
2. A reserve list, with expressions of interest that have passed the assessment thresholds. Those in the reserve list might be offered the possibility to become selected and thus, conclude a hosting and usage agreement, in case for whatever reason a hosting and usage agreement cannot be concluded with a higher ranked expression of interest or if additional funds become available.

In addition, the ECCC will draw up a list with expressions of interest that did not pass the assessment thresholds or were found to be ineligible.

The Executive Director will submit the final ranking list to the authorising authority with a proposal for selection of applications for its approval. Moreover, the Executive Director will in due course inform the ECCC Governing Board and the DEP program committee.

The authorising authority will make the final selection of applicants, who will be invited to conclude a hosting and usage agreement with the ECCC.

After the decision of the authorising authority, those submitting expressions of interest will be informed in written by the ECCC of the outcome of the assessment. The ECCC will also inform about the final selection or rejection of expressions of interest.

The ECCC will subsequently invite the selected applicants to the next stages for the signature of the hosting and usage agreement, and the preparation of the joint procurement(s) of goods and services for national SOC platforms, including the signing of a joint procurement agreement. However, the invitation does not constitute a commitment by the ECCC to launch the procurement procedures. The hosting and usage agreement, the joint procurement agreement, or any amendments to either agreements, must be approved by the authorising authority before they are signed by the respective parties.

6.3. Communication

The call document provides all the information required to submit an expression of interest. Please read it carefully before doing so, paying particular attention to the priorities and objectives of the call.

Any enquiries must be made by e-mail only to: CNECT-ECCC-DEP@ec.europa.eu.

Questions on submission must be sent before the deadline indicated in Section 7. The ECCC has no obligation to provide clarifications to questions received after this date.

To ensure equal treatment of applicants, the ECCC will not give a prior opinion on the eligibility of applicants, affiliated entity(ies), actions or specific activities.

Questions will be replied to individually. Questions and answers of broad interest and other important notices will be published (FAQ in English) at regular intervals on the European Cybersecurity Competence Centre website under the relevant call.

The ECCC may, on its own initiative, inform interested parties of any error, inaccuracy, omission, or clerical error in the text of the CfEI on the mentioned website. It is therefore advisable to consult this website regularly to be informed of any updates and of the questions and answers published.

No changes may be made to the expressions of interest once the deadline for submission has elapsed. If there is a need to clarify certain aspects or to correct clerical mistakes, the ECCC may contact applicants for this

purpose during the assessment process. This is generally done by e-mail. It is entirely the responsibility of the applicants to ensure that all contact information provided is accurate and functioning.

In case of any change of contact details, please send an email with the reference to the expression of interest and the new contact details to CNECT-ECCC-DEP@ec.europa.eu.

Applicants will be informed in writing of the results of the selection process. Unsuccessful applicants will be informed of the reasons for rejection. No information regarding the award procedure will be disclosed until the notification letter has been sent to the legal representative.

7. Tentative timetable

- 21 January 2025: deadline to submit expressions of interest to set up National SOC platforms and request for complementary grants under call DIGITAL-ECCC-2024-CYBER-07-SOC. **This deadline is definite, not tentative.**
- May 2025: finalisation of assessment of expressions of interest and grant application
- Q3 2025: signing of joint procurement/hosting and usage agreement
- Q4 2025: work with experts to draft technical specifications for joint procurement call(s) for tender
- Q1 2026: publication of joint procurement call(s) for tender by ECCC and cross-border SOC platforms
- Q2 2026: signing of procurement contract with selected contractors

8. Procedure for the submission of expressions of interest

Expressions of interest for joint procurement and proposals for grants must be submitted before the call deadline **21 January 2025 17.00 hours CET** (see also timetable Section 7).

Expressions of interest must be submitted electronically via the ECCC website using the **application form** available on the website under the relevant topic. Paper submissions are NOT possible.

Expressions of interest (including annexes and supporting documents) must be submitted using the forms provided with this call for expressions of interest that can be downloaded from the ECCC website and/or the **application form**. Section 4 provides information on how to fill in the submission forms.

Expressions of interest must be submitted in English, in the correct form, duly completed, and dated.

Your application must be readable, accessible and printable.

Proposals for grants must be submitted separately by responding to the call for proposals on the Funding and Tenders portal.[15]

Contact point for any questions is CNECT-ECCC-DEP@ec.europa.eu.

You have specific rights regarding processing of your personal data by the ECCC and the European Commission for the purpose of this call for expressions of interest. These rights are outlined in the Data Protection Notice available on the website under the relevant topic.

[15] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-eccc-2024-deploy-cyber-07-soc?isExactMatch=true&status=31094501,31094502&frameworkProgramme=43152860&callIdentifier=DIGITAL-ECCC-2024-DEPLOY-CYBER-07&order=DESC&pageNumber=1&pageSize=50&sortBy=startDate

Annexes

The annexes to this call for expression of interest are:

- Annex 1: **Information on the participant**
- Annex 2: I**nformation on the expression of interest** for the joint procurement(s)
- Annex 3: **Model hosting and usage agreement**
- Annex 4: **Commitment letter**
- Annex 5: **Blue-print architecture**

The following four documents (Annex 1 to 4) must be filled by applicants:

- Annex 1: **Information on the participant**
- Annex 2: I**nformation on the expression of interest** for the joint procurement(s)
- Annex 3: **Model hosting and usage agreement**
- Annex 4: **Commitment letter**

List of abbreviations

AI	**Artificial Intelligence**
CA	**Certificate Authority**
CEF	**Connecting Europe Facility**
CfEI	**Call for Expression of Interest**
CERT	**Computer Emergency Response Team**
CSIRT	**Computer Security Incident Response Team**
CTI	**Cyber Threat Intelligence**
DEP	**Digital Europe Programme**
ECCC	**European Cybersecurity Competence Centre**
EC	**European Commission**
ENISA	**European Union Agency for Cybersecurity**
EU	**European Union**
GB	**Governing Board**
HSM	**Hardware Security Module**
IoC	**Indicator of Compromise**
IPSec	**Internet Protocol Security**
ISAC	**Information Sharing and Analysis Centre**
JP	**Joint Procurement**
ML	**Machine Learning**
MS	**Member State**
OSI	**Open Systems Interconnection**
PKI	**Public Key Infrastructure**
SOC	**Security Operation Centre**
TCA	**Total Cost of Acquisition**
TESTA	**Trans European Services for Telematics between Administrations**
TLS	**Transport Layer Security**
VPN	**Virtual Private Network**
WP	**Work Programme**